Smart Card
Alliance

The Top 10 Hot Identity Topics

A Smart Card Alliance Identity Council White Paper

Publication Date: February 2006

Publication Number: IC-06001

Smart Card Alliance
191 Clarksville Rd.
Princeton Junction, NJ   08550
www.smartcardalliance.org
Telephone: 1-800-556-6828

About the Smart Card Alliance

The Smart Card Alliance is the leading not-for-profit, multi-industry association of member firms working to accelerate the widespread acceptance of multiple applications for smart card technology. The Alliance membership includes leading companies in banking, financial services, computer, telecommunications, technology, health care, retail and entertainment industries as well as a number of government agencies. Through specific projects such as education programs, market research, advocacy, industry relations and open forums, the Alliance keeps its members connected to industry leaders and innovative thought. The Alliance is the single industry voice for smart cards, leading industry discussion on the impact and value of smart cards in the U.S. and Latin America. For more information, visit http://www.smartcardalliance.org.

The Smart Card Alliance has used best efforts to ensure, but cannot guarantee, that the information described in this report is accurate as of the publication date. The Smart Card Alliance disclaims all warranties as to the accuracy, completeness or adequacy of information in this report.

Table of Contents

Executive Summary

Our shrinking world forces all of us to be constantly thoughtful of the need to protect our own identity and know with certainty the identities of those with whom we trust our wealth, our privacy, and our security. Protecting one's identity depends both on personal effort and on the practices, policies, and systems of the organizations to which one entrusts personal information. Individuals must exchange identity information and personal data almost daily with other individuals and with organizations. People constantly risk losing control of identity information and must rely on the entities that share the information to protect it.

With the increasing incidence of identity theft and increasing awareness of both the tangible and intangible costs to society of weak identity systems, individuals and organizations are taking more aggressive steps to secure personal information and to implement identity systems that improve identity verification processes.

To design and implement secure identity systems, organizations must think through the entire identity process and chain of trust. A complete identity solution must include policies, procedures, and practices that implement the desired level of security and that describe how people interact with the identity system. The solution must start with accurate vetting of the individual's identity and follow with identity verification processes that provide secure, authorized access to identity information. The technology selected is also critical; technology in general, and smart cards and biometrics in particular, are powerful tools that can help achieve overall system goals and enforce adherence to the chosen privacy and security policies.

This white paper was developed by the Smart Card Alliance Identity Council to provide a high-level discussion of the top 10 challenges associated with current identity systems. The paper covers a range of topics and offers perspectives on how the most critical identity issues can be addressed with policy, process, and technology solutions. The topics include the following:

- Discussing the actions government, businesses, and individuals can take to prevent identity theft and describing the role of technology in preventing theft.
- Describing both the institutional mechanisms and the individual actions that can keep an individual's personal identity information private.
- Defining what information constitutes an identity and how systems should be designed to put individuals in control of their private information.
- Assessing how governments respond to new technologies that can provide solutions to identity challenges.
- Analyzing the challenges posed by breeder documents and discussing potential solutions that could lead to more accurate proofing of an individual's identity.
- Discussing how a secure identity can be created and used throughout the identity life cycle.
- Defining the different types of identity credentials and offering guidance on key considerations for using a credential for multiple applications.
- Describing how new technologies are being used to verify an individual's identity in the online world.
- Defining how biometric technology is used in identity systems to bind an individual to an identity credential and verification event.

Secure, trusted identity systems will result only if policy, process, and technology issues are considered when new systems are being designed. The Identity Council's goal is to provide guidance on important identity issues, thereby helping policy-makers and implementing organizations understand how smart card and related technologies can best be applied to deliver the benefits of secure identity.

The Identity Council welcomes input from government, businesses, and the public. For additional information about Council activities, please visit http://www.smartcardalliance.org.

Introduction: Why Is Identity an Emotional Topic?

Many studies have attempted to define what a person's identity is. Some consider identity to be part of an individual's personality; others consider identity to be the characteristic that defines individuality and distinguishes one individual from another. This paper defines identity as the distinguishing characteristics that determine unequivocally that a person is who that person claims to be.

Human beings classify their surroundings by assigning names to the components of those surroundings. Everything has a name and everybody has a name. Naming is our way of ordering our world so that we can correctly address something or somebody. Knowing a person's name allows us to associate an identity with them, which in turn allows us to recognize whom we are dealing with and tell them apart from others.

Although people may want to maintain public anonymity, such anonymity is difficult to achieve. It is nearly impossible to maintain anonymity and operate in modern society. Birth certificates record our entry into society; Social Security numbers identify us to our government. We have passports to attest to our identity and citizenship; we have driver's licenses to show that we are considered competent to operate a motor vehicle. Each of these identity documents conveys our claimed identity to society for a specific purpose. Collectively, these documents form a series of reference points that attest to our identity. When we desire to achieve some form of anonymity, we use "personas" to represent us to a community where we wish to be less identifiable. For example, many people use personas on the Internet. By creating a "handle" or username in a web community, we can be invisible or not identifiable to some degree. Ultimately, however, the same individual is behind a real-world identity and the persona that the individual uses. Personas are simply a projection of a pseudo-identity masking the individual's actual identity. In many cases a persona may not be deemed sufficient identification to undertake activities such as financial transactions and therefore have limited use.

Although different people may define privacy differently, everyone would agree that it is important. Another critical point is the recognition that individuals should be in control of their identities. Personal choice should determine whether an individual discloses identity information. However, non-disclosure of one's identity may mean denial of a service to that individual. For example, the REAL ID Act of 2005 defines the requirements for identity proofing by states, who must issue compliant driver's licenses starting in 2008. The Act requires U.S. citizens who wish to access services such as flying on airplanes to present themselves and a compliant government-issued ID. Without such an ID, they will not be permitted to fly.

Identity is clearly a valuable commodity to an identity thief or a terrorist. By stealing another person's identity, somebody can cause a great deal of financial harm or gain access to services to which the thief is not entitled. Stronger ways of assuring and trusting identity are needed to prevent such theft.

Identity programs already affect how our society operates today.

- Many countries are beginning to issue electronic passports that include a smart card chip. These ePassports will deliver the passport holder's identity credential to an official accurately and securely. Such capabilities will make it more difficult to commit passport fraud or masquerade as somebody else. Passports will become a highly trusted credential for a citizen. Similarly, proposals are being considered for identity cards for citizens who routinely cross U.S. land borders. These proposals include requiring a biometric identifier, to ensure that the person presenting the card is truly the owner of the card.

- The U.S. Government is committed to satisfying President Bush's Homeland Security Presidential Directive 12, which requires all government employees and contractors to be issued a credential that will be interoperable across the entire Federal government. By October 2006, every agency is required to start issuing smart card-based identity cards conforming to Federal Information Processing Standard 201. Biometric identifiers will form the foundation for identity verification. With the use of smart card technology and privacy-enhancing biometric templates, the person's biometric can be matched locally, either on the card itself or in the local terminal, eliminating the need to go online to biometric databases for every verification.

- Plans to issue identity cards to frequent, trusted travelers is another example of how a person's identity will be presented to gain access to a specific service – in this case, access to expedited security check lines at airports. These cards are also likely to include biometric identifiers to bind the user to their credential.

Summary

Identity presentation is one of the most important aspects of modern society and is an important part of a person's life. As we embrace the information age, where data is a valuable commodity, it is essential to use adequate security techniques to preserve each person's identity and privacy.

A citizen is entitled to identity protection. A person's identity should remain private and be disclosed in a secure and trusted form only when the person chooses and only to whom the person chooses. The party receiving the presented identity should be able to verify that the person presenting the identity is the person entitled to present it, and the credential itself should be authenticated. Once we establish a chain of trust for identity, many areas of our society will benefit. Electronic commerce (ecommerce) can become a trusted transaction environment. The nation's transportation infrastructure will become secure, as travelers are better identified, making it exponentially harder for a terrorist to gain entry using a false identity.

The Smart Card Alliance recognizes the importance of identity in society and the critical need to protect it and be able to trust it. Smart card technology has proven itself to be a valuable tool for achieving these goals.

In the following pages we explore 10 of the main identity challenges facing our society today.

Identity Topic #1: Identity Theft—When You Don't Own Your Identity!

Introduction

An individual's identity is defined most simply by the set of characteristics that enable a person to be recognized or known. There are three ways of thinking about identity:

- Identity from nature: characteristics given by the birth parents to the child (fingerprints, DNA, iris pattern)
- Identity from status: characteristics assigned to individuals by other people in society (Social Security number, credit card number)
- Identity from behavior: characteristics assigned to individuals by other people based upon the individuals' actions (marking profile, credit rating, criminal record)

According to the U.S. Federal Trade Commission, identity theft is the nation's fastest-growing crime in the United States. By many accounts, it is the fastest-growing crime globally.

What Is Identity Theft?

Identity theft is the appropriation of another person's personal information without permission in order to commit fraud, to steal the person's assets, or to pretend to be the other person. Identity theft is the fastest-growing crime in the United States, according to the U.S. Federal Trade Commission (FTC). Between January and December 2004, Consumer Sentinel, the complaint database developed and maintained by the FTC, received over 635,000 consumer fraud and identity theft complaints. Consumers reported losses from fraud of more than $547 million.

There are many types of identity theft, and many stakeholders besides the perpetrator and the victim are involved in identity theft. Identity theft affects all of society.

How Does Identity Theft Occur?

To prevent identity theft, it is essential to understand who commits identity theft and how identity theft occurs. Typically, three types of people commit identity theft:

- Someone close to the victim, who knows the victim's habits and movements
- Amateurs, who look for unsuspecting subjects and opportune moments
- Professionals, who work independently or as part of an organized group.

There are many ways to commit identity theft, some simple and some very sophisticated. Simple methods are used mostly by persons close to the victim and by amateurs. The most common simple methods are dumpster diving and social engineering. Dumpster diving is the practice of rummaging through garbage for a consumer's personal information. Dumpster divers rely on the fact that people are not aware of the value of the information they possess and are careless about protecting and discarding it. Social engineering methods generally use techniques that rely on human interaction to trick people. A perpetrator might try to gain the confidence of a colleague and then ask to "borrow" their user ID and password to access a secure network, or they might impersonate a utility representative and call an unsuspecting customer to "verify" the Social Security number associated with the account. There are countless examples of these simple methods, and even in today's environment, they remain very successful.

Professionals use both simple and sophisticated methods to steal identities but tend to focus on methods that can be automated since such methods can be less time-consuming and more profitable. These automated methods are usually technology-driven and include techniques such as skimming, hacking, phishing, and pharming.

- *Skimming* is the practice of stealing credit card information by capturing it in some form of card reader. The thief employs methods such as swiping the credit card a second time during an actual purchase or attaching a reader to an ATM machine where the card is swiped. Skimming occurs infrequently because of the technology required, but when it does occur, damages can be substantial.
- *Hacking* is the act of gaining illegal or unauthorized access to a computer system or network. Hacking is the most commonly used method for stealing an identity. Spyware on a computer can be considered hacking, even though the user may have authorized installation of the spyware. Spyware is defined as programs such as keystroke loggers and screen capture utilities, installed by a third party to monitor and observe online behavior or capture passwords and other information. Applications such as adware install themselves surreptitiously through “drive by” downloads or by piggybacking on other applications. They track users’ behaviors and take advantage of their Internet connection. Users often unknowingly authorize spyware to be installed by clicking on the “Yes” button at the bottom of an end user license agreement.
- *Phishing* is a cyber attack that directs people to a fraudulent website to collect personal information. A common phishing scam is to send an email message asking a user to update an account. The perpetrator uses an attractive lure—protecting privacy—and then asks users to verify their accounts by clicking on a convenient hyperlink. A phishing scam may also lure an individual by sending an alarming message stating that a desired service is about to be terminated. Phishers often use the services of spammers to reach the widest number of possible targets. There have been literally thousands of phishing scams on the Internet.
- *Pharming* is a cyber attack that involves a combination of ploys such as phishing, viruses, spyware, and domain name system (DNS) server cache-poisoning or spoofing. Pharming directs people to a fraudulent website by poisoning the DNS server so that web requests are redirected. Victims think they are entering personal information on a legitimate site when in fact they are not. A pharming site will often forward the web request on to the legitimate site so users see their real data. By monitoring the traffic between the user and the intended site, a pharmer can eavesdrop on personal information and even manipulate transactions.

What Actions Are Government Taking against Identity Theft?

The Federal government and many state and local jurisdictions are passing laws and regulations requiring businesses to take certain actions against identity theft and to establish guidelines for notifying consumers when data breaches may have occurred. Governments are promoting consumer education and resources for preventing and, where necessary, recovering from identity theft.

What Are Businesses Doing to Prevent Identity Theft?

Identity theft causes substantial financial harm to private industry. Businesses incur costs to implement identity theft prevention measures and to replace the losses suffered by the victims of identity theft. These costs are absorbed by the industry and by insurance companies, but eventually they are passed on to the consumer in the form of higher prices for products and services, higher fees, and higher interest rates. Different industry sectors are tackling this problem in the manner most appropriate for that industry and for the specific patterns of theft. Being proactive, staying ahead of the professionals, and being current and diligent in security and privacy protections are critical.

How Can Technology Help to Prevent Identity Theft?

Technology measures can prevent some types of identity theft. Businesses can require multi-factor authentication (two indisputable sources or elements that must be supplied to verify a person’s identity). Smart card-based implementations can be adopted, such as subscriber identification modules, which prevent cloning of phones and have eliminated telephone theft/fraud, or smart card-based employee IDs, which provide strong authentication, are difficult to counterfeit, and are tamper-resistant. Human intervention and resistance are required to successfully attack non-technical methods of identity theft such as dumpster diving and social engineering. In the case of dumpster diving, for example, a paper shredder can be used to destroy paper bills.

What Should Consumers Do to Protect Themselves?

Consumers should be aware of their rights and responsibilities for protecting themselves and request a free copy of their credit report. In the U.S., a recent amendment to the Federal Fair Credit Reporting Act requires that the national consumer reporting companies (Equifax, Experian, and TransUnion) provide consumers with a free copy of their credit report, upon request, once every 12 months. Consumers need to make this request through the FTC website, as this is the only authorized online source. Consumers are urged to monitor their reports routinely for unusual activity. Consumers are also encouraged to be proactive:

- Stay educated about the value of identity characteristics.
- Monitor sources of identity for possible abuse or misappropriation.
- Develop an attitude of caring about identity as a personal asset.

Identity Topic #2: Protection of Identity Information—Is Your Identity Protected? Can You Protect It?

Introduction

Protecting one's identity depends both on personal efforts and on the practices, policies, and systems of those organizations to which a person entrusts personal information. Daily life requires individuals to interact with other individuals and with organizations and, in the process, to exchange identity and other personal information. People constantly risk losing control of identity information and must rely on the entities that share the information to protect it.

The increasing incidence of identity theft has led to an increasing awareness of the need to protect identity information. As a consequence, both individuals and organizations are taking more aggressive steps to secure personal information. Concurrently, a number of laws and regulations have been put in place to ensure that personal information is protected and secured. The threat of litigation and financial penalties are motivating organizations and individuals to institute appropriate mitigating measures.

As the result of legislation and the threat of litigation, both the public and private sectors are instituting new policies and practices designed to protect identities, ensure privacy and control access to identity information.

Laws and Regulations

A number of new U.S. Federal and state laws and regulations have recently passed (or are pending) that address the risk associated with organizations not adequately protecting the identity data in their custodial care. These mandates address policy and business practices as well as ensuring that appropriate operational and information technology security measures are instituted.

One piece of legislation that was recently passed specifically to address the identity theft issue is the California Security Breach Information Act (SB 1386), which requires commercial organizations to notify their customers whenever they suspect the security of a customer's data has been compromised. This notification is required regardless of whether there is evidence that an individual's data file has actually been compromised. The Act also requires across-the-board notification if only one person's file has been affected. The consequences for not complying with the notification requirement include financial penalties, negative publicity, and the risk of multiple civil lawsuits. These negative consequences create a strong incentive for affected companies to comply with the law. A bill has been introduced in the U.S. Congress modeled after the California law. The bill is still in conference but could become law sometime over the next few years.

Other laws that directly affect privacy protection in the U.S. include Sarbanes-Oxley, Gramm-Leach-Bliley, and the Health Insurance Portability and Accountability Act. The common theme of all these laws is that sensitive information, be it personal, medical, or corporate financial, needs to be protected to prevent restricted or private data from being accessed by unauthorized individuals or organizations.

Corporate Policies and Practices

More corporations and private sector organizations are modifying their business practices, operations, and policies to enforce the protection and appropriate use of private data. Certainly anyone who has a brokerage, banking, or credit card relationship with an institution has received privacy notices that describe how the institution protects and uses the private data entrusted to them to facilitate business-consumer transactions.

One hallmark of these policies is the assurance provided to individuals that their private information will be protected and used only to support the delivery of services; indeed, this type of assurance is often promoted as a differentiator between competing organizations. Polls show that security and protection of information are key reasons why consumers choose one business over another, and the private sector is catering to this concern by including it in marketing and advertising campaigns.

In addition to policies, corporations have implemented business practices and processes that authenticate the identities of the people with whom they transact business to ensure that imposters and fraudsters are not granted access to sensitive information. Examples include fingerprinting people when they cash checks, using multi-factor authentication for web-based and face-to-face transactions, and employing layered security techniques to assure correct and reliable enforcement of access control privileges.

Government Policies and Practices

The U.S. Federal government has also instituted a number of policies and regulations designed to protect privacy and heighten security for the storage and use of personal data which it protects as a custodian. A number of initiatives under such headings as E-Authentication, FISMA/GISRA, and the Privacy Act now govern how the government collects, uses, and stores identity information. New access controls are being instituted and enforced, for both internal access by employees and access by the citizenry, and security measures are being increased to ensure the protection and privacy of stored information such as Social Security records and medical files.

Often, government initiatives to protect data and ensure privacy have led the way for similar programs in the private sector. Because the government manages some of the largest databases and identity systems in the world and is under constant public scrutiny, it is not surprising that it is leading the way in implementing policies, practices and technologies designed to protect identity and enhance privacy.

Individual Behavior: Steps You Can Take

Protecting one’s identity is not just the responsibility of governments and corporations. Individuals have an important role to play in protecting their own identities by taking appropriate, cautionary measures. There are a number of basic rules that individuals should follow, such as:

- Shred or destroy trash that contains personal information (e.g., bank statements, credit card statements, bills).
- Do not provide personal information to suspicious websites or individuals who contact you using email. The same rule also applies to telephone and mail communications. Thoroughly investigate and determine the authenticity and legitimacy of any person or organization that contacts you asking for personal identity information.
- Be cognizant of how your identity credentials are used; make sure that your driver’s license, credit cards, and other credentials are not misused during transactions. Try not to let them out of your sight and maintain control of them to the fullest extent possible.
- Report lost or stolen credentials to the appropriate issuing authority immediately.

Identity Topic #3: Who Are You?—The Confusion over Identity Information and Determining Who You Are

Introduction

Who are we? In a societal context our identity is established through a series of events and relationships, starting with one's birth, along with the resulting documentation. Our identity is represented to others through a patchwork of this identity documentation – original paper documents (or copies), ID cards, driver's licenses, passports, and other types of credentials. In today's world, managing these items and keeping them safe is an increasingly difficult challenge for all of us.

Identity is represented by an assortment of information that can be tied to that individual and that describes an individual's characteristics and uniqueness.

How Many Identities Do We Have and Need?

All of us have and use numerous identities in our everyday lives. Some examples are:

- *Professional identity*: identity information used by employers
- *Financial identity*: identity information used by financial institutions, such as credit card information
- *Citizen identity*: identity information used by governments, such as passport information.
- *Healthcare identity*: identity information used by the healthcare industry
- *Online browsing/email identity*: identity information used to access information on the Internet, such as usernames and passwords
- *Ecommerce identity*: identity information used to carry out electronic transactions, such as account numbers, passwords, shipping addresses and credit card information

Technological and process solutions are available that can create more manageable and secure identity tools. Adopting these solutions can ease the fears we all have about identity theft and fraud and implement more efficient identity transactions. To understand these solutions, however, we must understand some of the challenges that underlie the concept of identity.

What Is Identity?

Identity is represented by an assortment of information that can be tied to that individual and that describes an individual's characteristics and uniqueness. An identity in this context is the information concerning the person, not the actual person.

An identity can be made up of many pieces. Some common components of identity are:

- *Demographics*: information describing who you are (name, address, phone number)
- *Biometrics*: information measuring a person's physical or behavioral characteristics (e.g., fingerprint, face, iris, hand, speech)
- *Actions*: information describing what you do and/or where you go
- *Preferences*: information describing what you like or choose to buy
- *Status*: information describing your social status (member or nonmember, married or single, retired, grade level)
- *Transactions*: information describing a person's past transactions (financial credit status)

Current Identity Systems: Multi-use or Silo?

Identity systems have proliferated in today's society. Some of these systems have developed into multiple-use identity systems while others remain essentially identity silos - single-use closed systems. The more applications a collection of identity information has and the more meaningful that information is to third parties, the more valuable that identity information becomes. The U.S. driver's license is an example of a multi-use identity tool. Its primary purpose is to prove driving status but it can also be used to provide evidence of identity when opening a bank account, buying alcohol, boarding an airplane, or applying for a job. Another example of a multi-use identity system is a major credit/debit card. Holders of these cards can use them to purchase goods and services almost anywhere in the world. Other collections of identity information have limited use and are essentially identity silos, such as healthcare cards, single-retailer discount or member cards, single retailer credit cards, and online subscriber account information. Although this identity information is more limited in scope than multi-use information, it is less likely that this identity information will be revealed outside of the system in which it is used. For example, healthcare information may be less likely to be divulged to those not needing to know if it is kept within one identity system. Of course, the problem of privacy is not solved by putting identity information in silos. It must be emphasized that identity information is only as secure as the system designed to manage that identity information. Identity information that is in a siloed system is less likely to be divulged outside the system only because it is used and transported less often than information in a multi-use identity credential.

Putting the Individual at the Center of the Identity System

Because it is important for individuals to maintain control over their private identity information, it is necessary to understand where the individual fits in the general identity system structure. There are generally three parties to an identity system:

1. Identity system providers: Entities that proof information, enroll individuals, and issue identity credentials. For example, governments provide identities to citizens through passports or visas.
2. Identity system members: The people who must use identity information to obtain privileges. For example, an individual uses the ID badge issued by an employer to enter a secure facility.
3. Identity system users: Organizations that rely on identities and credentials (banks, law enforcement, retailers). For example, an employer uses a person's driver's license or passport as proof of identity for a job application.

As we can see, the individual is indeed at the center of the identity system – or maybe more aptly put – stuck in the middle. With identity system providers responsible for collecting, verifying, and storing identity information, and identity system users clamoring to get access to this data, it's no wonder that individuals get nervous about their identity information. So what to do? Well, some of the main concerns that we all have regarding identity systems can be addressed by incorporating robust and auditable policies, practices and processes into our identity systems. The following are some guidelines to use when creating an identity system:

- *Consent*. Establish identity systems that enforce a policy of consent when transferring identity information. Identity systems should only reveal information identifying a person with the person's consent. The information should be limited to the information that is necessary to complete the transaction.
- *Transparency*. An individual should be able to "see" how identity information is being used. Although individuals may not be authorized to modify transaction information, both they and the entity they are interacting with are best served if the information is visible to them. Visible information creates a higher level of trust between the individual and the entity and also creates a feedback security loop to help individuals police the use of their identity information. (For example, credit card companies allow their customers to access a list of monthly transactions. Fraudulent credit card transactions are often reported by the customer.)
- *Privacy and security*. Incorporate privacy and security features as fundamental and pervasive elements of the identity system.

- *Interoperability*. Make the identity system interoperable, so that the individual can use the identity information broadly.
- *Biometrics*. Use biometrics as an integral part of the identity system, so that a person is physically associated with the identity information and the identity credential.
- *Ease of use*. Adopt ease of use as a primary design principle. The user experience should be simple and consistent. Automating transactions to reduce time and complexity is an important consideration.

Identity Topic #4: Is Technology a Threat to an Individual's Identity?

Introduction

Our shrinking world compels individuals and societies to be constantly thoughtful of the need to protect our own identities and to know with certainty the identity of those with whom we trust our wealth, our privacy, and our security. When confronted with new opportunities for increased commerce, freedom of movement, communication, and knowledge, we've almost always chosen to move forward and have repeatedly turned to technology to enable us to do so and to protect us against the threats accompanying these new opportunities.

All changes to the status quo entail costs and risks. The challenge is to find ways to make informed decisions about the costs, risks, and benefits of using new technologies to protect our identities. The process we use to evaluate new technologies is critical to achieving benefits from their adoption.

When our governments consider the hazards and benefits of society's adoption of a new technology protecting our identities, legislating against its use instead of making illegal its misuse will inevitably "throw the baby out with the bath water," depriving society of the technology's benefits.

What Has Technology Done for Us Recently to Protect our Identities?

Reliable identification is critical to transactions between parties who have inadequate knowledge of each other. The success of such transactions relies on a trusted third party being able to vouch for the participants' identities. Third-party testimonials are used in face-to-face transactions of all kinds and in remote transactions, such as purchases over the phone and the Internet. The identity credential issued by the third party must be portable; otherwise, we would constantly be relying on in-person validation like that performed by a notary, something that is inconvenient, costly, and time consuming.

Technology has been able to improve and protect our transactions with strangers and our personal information in a variety of ways. Technology makes such transactions faster, more secure, and more convenient (for example, contactless payment systems like American Express® ExpressPay) and makes access to personal information more secure (for example, biometric authenticators like fingerprints and iris scans). Credentials containing our identities (for example, the new U.S. electronic passport containing a chip) are made more secure by using smart cards that employ the latest cryptographic methods to protect the data on the card and authenticate the entity accessing the data. Smart cards are also being used to protect access to our personal information over public and private networks. These are just a few examples of how technology is being used today to help individuals protect their personal information.

Who Controls When New Technologies Are Adopted?

In our private lives, technological solutions for protecting our identities or increasing our ability to interact more easily with others are typically adopted incrementally. Trade-offs among security, privacy, convenience and cost are continually balanced and rebalanced by mechanisms of our free markets. Some people choose to adopt new technologies immediately, while others choose to wait until the technology is "proven." We decide when the time is right for each of us.

Currently, our society as a whole is faced with threats to its physical security posed by the falsification of identities at the state and Federal level, and government is charged with addressing these challenges. However, any technological solutions that are chosen to combat these threats cannot be imposed incrementally. The implications of implementing a new technology throughout an entire society are far reaching, and we need to understand and balance the tradeoffs between security, privacy, convenience, and cost immediately.

Don’t We Need Laws to Control Adoption of Technology Protecting our Identities?

With technology becoming more prevalent and complex and with the pace of change accelerating, governments are struggling to keep up with new threats to their citizens’ identities. Two legislative alternatives commonly considered in such situations are to:

1. Legislate against new technologies until they are adequately “proven” or deemed safe; or
2. Outlaw the willful misuse of new technologies, and legislate the responsibility for damages in the event of failures with no criminal intent.

The first approach carries the genuine risk of “throwing the baby out with the bath water” and depriving society of the benefits of a new technology. The latter allows the benefits to accrue to society without locking in the status quo or selecting technological favorites that can result in stifling competition and increasing costs to society.

How Should Governments Decide Whether to Enact New Laws Governing a Technology?

A new technology that protects our identities is by nature complex, and reaching a full understanding of its benefits, risks to citizens’ privacy, and vulnerabilities is difficult. Only by involving a wide range of experts and balancing all the pros and cons can logical decisions be made.

- Identity technologists – to explain methods of operation, limits on performance, financial limits on enhancement, and types and likelihood of misuse.
- Privacy and consumer advocates – to identify the risks associated with the use and possible misuse of a new technology.
- Policy experts – to identify how the technology can and should be used procedurally.

Any decision reached without the involvement of all of these parties in an open forum will invariably result in skewed decisions that may deprive us of the proper benefits of the technology.

It is most important, however, to keep in mind that technology is merely one part of the solution to the problem of protecting our identities and validating them to others. The complete solution is a system that must include policies, procedures, and practices describing how people are to interact with the system. In the end, the strength of a system is only as great as the adherence by the people using the system to these policies and procedures. Technology in general, and smart cards and biometrics in particular, are powerful tools for enforcing adherence to policies and procedures.

Identity Topic #5: How Do You Prove Your Identity?—The Problems with Breeder Documents

Introduction

A breeder document is so named because it is usually a source of identity to apply for (or breed) other forms of identity credentials.

A number of years ago, Australia embarked on a project to digitize all birth, death, and immigration records and maintain them centrally as electronic records. The thinking was "if you are here, you were either born here or you came here, and thus there should be a record on you." In the United States, an E-Government project known as E-Vital was initiated to digitize and make available some of the same kinds of records. However, only death records are currently (mostly) centralized and electronically stored, as a result of the Federal government paying the states to digitize death certificates. Progress on automating other vital records has been very slow. Birth, death, marriage, divorce, and other records may be both issued and maintained in multiple places. At best, such records are automated and maintained at the state level; at worst, they are not automated and are stored in counties across the country.

The Challenge with Breeder Documents

Australia is a good example to use to consider the concept of providing a secure and verifiable identity for every person in a country. Suppose that Australia decided to issue a national ID card to all of its residents. Australia certainly has the technology needed to produce a credential that could include biometrics, the issuer's digital signature, and PKI certificates. Such a credential could properly be viewed as very secure and be tied to the holder in a way that would make it very hard to counterfeit or alter.

By issuing such a credential, Australia would solve half the problem: a central database would confirm the existence and legal presence of every credential holder. The other half of the problem would remain unsolved, however: how to be certain that the person who presents a birth certificate or other "breeder" document to obtain the credential is the true owner of that document.

The Australian example illustrates the obvious problem for the United States. The United States can automate a record system and put records in a central place. A central database can be queried to verify a person's existence and permit a very secure, biometrically linked credential to be issued. However, two very important things cannot be done:

1. The authenticity of the documents presented to establish identity cannot be validated.
2. The individual presenting a document cannot be tied to the document.

Most documents simply do not have enough built-in security to be verified, and few documents can be tied to the individual presenting the document.

In general, this problem is true of most of the documents used to establish identity in the United States, with the exception of the passport and the alien registration card. These documents, which are at the top of the identity food chain, are the product of an identity proofing or adjudication process and contain a variety of security features that can be authenticated and that make them virtually tamper-proof.

However, the identity vetting process that precedes issuance of even these documents relies on much less secure documents: birth certificates, driver's licenses, Social Security cards, and foreign passports. The acceptance of documents that may not be genuine or of genuine documents that are not the property of the presenter can result in the issuance of a highly secure credential to an individual other than the individual identified by the breeder documents and a false sense of security in the identity verification process.

The United States has a breeder document problem that it is nowhere close to solving and that may not ever be solved. We do not have databases that can be accessed to determine whether a person actually exists. We do not, for the most part, produce birth certificates, social security cards, or, in some cases, driver's licenses that can be authenticated. We do not have the ability to tie most of these breeder documents to the bearer biometrically.

The Root of the Problem

The birth certificate is both the start and the heart of the problem. Over 100 million birth certificates are issued in this country each year, and in about a dozen states, they are public documents available to anyone who wants a copy. Even in states that ask for some indication of entitlement the controls are very weak. We cannot readily verify the validity of a birth certificate, nor can we be sure that it belongs to the person presenting it. Very good false birth certificates are readily available over the Internet or (in certain geographical areas) from open document markets. These birth certificates can then be used to obtain other legitimate documents, such as driver's licenses, Social Security cards, and potentially even passports. Most issuers of legitimate documents have made little or no investment in the few available technologies that could help them detect bad breeder documents. For example, virtually no organization other than the U.S. Department of State has been willing to incorporate chip technology into documents issued to members of the public.

Possible Solutions

Solving these problems can be expensive, and the solutions could take many years to implement. Some are sure to raise sensitive issues regarding identity information. One of the more comprehensive solutions involves capturing DNA, tying it to a birth certificate, and linking other biometric information (such as facial images, fingerprints, or retinal images) to the DNA. Another option is to require that older documents be reissued and tied to a rigorous identity-proofing process before a driver’s license or passport can be obtained. These solutions may require that national standards be set for a variety of documents issued by state and local governments. Perhaps most difficult and controversial of all, such solutions could involve the creation of central databases that contain not only vital records but also biometric measures that tie the records to a specific individual. Such databases could be used to verify not only the existence of a document but also that the presenter is the true owner of the identity to which the document attests**.**

A more workable interim solution may be to require new identity document applicants to go through a rigorous proofing process that attempts to thoroughly validate the information on current breeder documents. This proofing or vetting process can be a combination of authenticating the physical breeder document, contacting the issuing authority to verify the individual’s claim to the breeder document, checking other pubic and private database sources for activity on the identity information, and cross-checking the demographic information in these databases for matches. As more data sources are checked, the probability of a valid identity is higher. See topic number 6 in this paper for a more detailed discussion of the options for identity proofing and verification.

Conclusion

Breeder documents are a challenge that at some point must be faced. Ignoring this challenge can only compromise the security of any identity system. Even governments with the money and the political will to start down the path to a solution now, however, will find that the path is lengthy and twisted. But there are feasible solutions, combining both procedural and technical elements, that can bolster current breeder document systems, and more radical alternatives are available for replacing or redefining certain breeder documents. All of the breeder document issues must be examined soon, so that a plan to further secure citizen identity information can be implemented.

Identity Topic #6: Verifying a Person's Identity—Are You Who You Claim To Be?

Why Is a Verifiable Identity Important?

Identity information in and of itself is not that valuable if it cannot be readily verified. Once an identity relationship has been established, for example enrolling in a club, it is the verification of membership that grants access to member privileges. Some privileges, like getting a discount card from a retailer or creating an email address with an online provider, are simple and do not require extensive identity verification. Others, like getting a passport or a mortgage, are more valuable and require more comprehensive identity verification. Organizing identity information in a unique, verifiable, secure, and reliable format, such as in an identity document or credential, is a basic tool for efficiently accessing privileges and transacting business in society today.

In today's world of automated access control and online commerce, your identity won't get you far if it can't be readily verified.

What Makes an Identity Secure?

A secure identity is the verifiable and exclusive right to the exclusive use of the identity information being presented by an individual for the purpose of gaining access to a set of assigned privileges. A secure identity can exist in both the physical world and the digital world.

Securing identity, in this context, is a topic of great interest because of the potential for harm to individuals and society that misused identities present in today's world. Securing an identity for exclusive use means that the identity information must be hidden from those for whom it is not intended and bound exclusively to one individual.

A Secure Identity Transaction

Transactions in which a secure identity is presented can require the following:

1. A credential (physical or digital) containing identity information.
2. A biometric measurement (a fingerprint, for example) that is compared to biometric information contained in the credential or to stored biometric information.
3. A piece of secret information that the person knows, that is understood by the observing party (a password, for example), and that is not contained on the credential.

In other words, a secure identity transaction involves the following:

- Something you have (a credential).
- Something you are (a biometric factor).
- Something you know (a password).

One of these elements by itself is not generally enough to guarantee a highly secure transaction; used in combination however, they create a high level of assurance that a person is who that person claims to be. But creating secure credentials, capturing biometric information, and requiring memorized passwords introduce complexity and cost for all parties.

The Identity Life Cycle—Creating a Secure Identity

We all go through the steps required to create a secure identity at least once in our life time. The typical steps in an identity life cycle include:

1. Have identity information vetted.
2. Enroll the identity information in a system, creating a record that has privileges associated with it.

3. Create an identity document or credential.
4. Use this credential to access associated privileges.

The first three steps result in a secure identity relationship with an entity. The fourth step allows an individual to present or assert an identity. This cycle can be repeated over and over throughout our lives to create identity relationships and gain privileges.

Step 1: Vetting an identity

Before enrolling an individual in a system, it is critical to verify that the person is who the person claims to be. Although this task may be cumbersome, it is critical to the success and security of the entire identity system. How rigorously a person's claimed identity is examined should depend on the value of the privilege being granted or the potential harm that could be caused by allowing a fraudulent identity to access the privilege.

Thoroughly proofing an identity can include the following:

1. Cross-checking all identity documents offered by an individual.
2. Verifying the information on all documents with the original issuing authorities.
3. Verifying elements of an identity (such as names, addresses, phone numbers) with third parties.
4. Checking the identity information against watch lists of known criminals or fraudulent activity information.
5. Matching existing biometric information with the individual's biometric information.

If any parts of this proofing exercise do not support the identity claim, the effort to link the person to the claimed identity can either be escalated, requiring further investigation and additional proof of identity from the person, or the person can be denied a credential.

Step 2: Enrolling and Privileging

After an individual's identity has been verified, the appropriate identity data for that person needs to be entered into a database record and associated with the privileges being granted. This is when identity privacy is a concern. The identity data recorded is private information being held by the organization granting the privilege.

Step 3: Issuing an Identity Credential

Even though the first three steps of the life cycle may all occur at the same time and place, the issuance process itself must be secure (e.g., protecting access to the identity information during issuance and using secured facilities to protect physical access to both data and material). A secure credential should also include the following elements:

- Both visible and hidden security features
- A structure designed to last for the duration of the privilege
- Tamper- and copy-resistance, to reduce fraud
- Unique and secure design features
- Automated authentication features
- Visible and hidden identity information, to segregate public and private identity information
- A biometric identifier, to bind the credential to its owner

Step 4: Use

A secured credential is issued so that the person who is tied to the credential can access the privileges associated with the credential. Ease-of-use considerations, such as the speed at which the credential can be used in an authenticated transaction, are important. So is the durability and visual clarity of the credential. Another key consideration is the protection of private information on the credential from unauthorized access when the credential is used.

Summary

The importance of the first step in the identity life cycle cannot be overemphasized. Unless an individual's identity is thoroughly vetted to assure that the person is who the person claims to be, the credential and the entire system are at risk for misuse. The risk of losing what is being protected must be balanced against the cost of creating and maintaining both a secure identity credential and the systems that support it.

Identity Topic #7: Identity Credentials—What's in a Credential?

Each type of credential has particular usage and privacy characteristics.

Discussions about identity frequently include references to the concept of a single all-purpose identity credential or, more realistically, a small set of multi-function use credentials. To determine how practical or desirable this concept is, it is useful to review the purpose of credentials and how credentials are used.

What Is a Credential?

An identity credential holds information that grants an individual access to predetermined permissions or privileges. These might include physical access, access to computers, permission to enter a country, or permission to vote. An identity credential also links the credential holder to the permissions they use, allowing transactions or events to be associated with specific individuals. Commonly used identity credentials include the following:

- Passports
- Visas
- Alien residence cards
- National identification cards
- Voter identification cards
- Driver's licenses
- Employee IDs
- Student IDs
- Social benefits cards
- Birth certificates
- Library cards
- Transit passes
- Membership cards

Each kind of credential has particular usage characteristics. These characteristics are determined by the authorities and systems that issue and use the credential. Some of the issues they must contend with include:

- Who issues (owns) the credential
- Who can invalidate the credential
- Who determines what is printed on the credential
- Who can load and update the credential
- How is the credential used and validated
- How is the credential updated, and how often
- How long is the credential valid

Each kind of credential also has particular privacy considerations, determined by the information printed or stored on it. In some cases, especially if the credential is machine-readable, the credential and the credential reader can authenticate each other to ensure that both can be trusted. This can enhance privacy protection for the credential holder (and improve the security of the system using the credential).

Each kind of credential has an associated degree of value and security measures. A counterfeit or altered library card or bus pass does not contain much value or pose a great risk to society.

However, a counterfeit passport or employee ID that grants access to government computers could have grave consequences. Systems that use credentials, especially high security systems, must be able to determine that:

- The credential was created by the legitimate issuing authority.
- The credential has not been altered.
- The bearer is the rightful owner of the credential.

There are a number of technologies that can help achieve this level of trust. Security printing, tamper-evident topcoats, covert security features, biometrics, secure integrated circuits (ICs), and cryptographic techniques are some of the technologies available. All of these features can enhance privacy and security, and thus the level of trust, in a credential system. But all of these features cost money. Some of the trade-offs that should be weighed when considering these features versus their cost are:

- Should low security applications or systems be burdened with the expense and overhead of a high security credential?
- Should credential issuers allow their high security credentials to be used in low security applications or systems?

Updating a credential raises additional concerns:

- Who can update the credential, and under what circumstances?
- Who is responsible for data integrity?
- How will a lost or damaged credential be replaced?

Multi-Application Credentials

The major decision to make when issuing a multi-application credential is which applications should be included on the credential. The following multi-application credential examples illustrate key considerations for the types of applications that should be combined.

There are already various implementations of the multi-application *electronic purse*, which has one owner – the issuing bank. All applications on the credential are cash replacement applications, such as ATM withdrawals, parking fee payments, transit payments, and other payment applications.

A national identification card is an example of a multi-application credential. Depending upon a country's social structure, it can be logical to group a number of government-sponsored applications such as national identity information, social benefits, health care, and licenses on one card issued and "owned" by the government. For convenience, an epurse application might also be added. The Malaysian national ID is an example of such a card.

Some *employee IDs* already provide for multiple levels of physical access and access to computer networks. The U.S. Government's new Personal Identity Verification card for government employees and contractors is another example of a multi-application credential. In some cases, adding company-sponsored healthcare information might be logical.

Passports, on the other hand, are a good example of a single-application credential. Passport systems have very high security requirements. The credential lasts for 5 or 10 years, and data can only be added or modified under the control of the issuing state. With time, perspectives may change, but to date no countries issuing the new electronic passport are considering additional applications.

Smart card technology can support a variety of multi-application credentials. The operating systems are very secure and offer cryptographic functions that guarantee separation of applications. Critical data can be cryptographically signed and, if necessary, encrypted for additional security and privacy. Access privileges are enforced by the operating system and can vary by application.

Identity Topic #8: Use of Identity Information: The Importance of Privacy Principles

Fundamental to any identity management system is trust: trust that the identity information contained within the system is accurate and will be used only for the purposes for which it was collected. If individuals fear that their identity information could be inappropriately shared or used, would they trust the identity system?

Because identity systems are the custodians of large amounts of personal information, it is important that they embrace rigorous privacy principles.

Privacy Principles

Since the 1970s, the U.S. Federal government has recognized the importance of maintaining trust and transparency in systems that contain personal information. In 1973, the Department of Health, Education, and Welfare, the predecessor to the Department of Health and Human Services, issued *Records, Computers and the Rights of Citizens,*[1] a report that recommended the adoption of a Code of Fair Information Practices. The Code rests on principles which can be summarized as follows: *no information collected about an individual should be kept secret, and individuals should have access to and notification of the use to which their information is put in order to prevent data inaccuracies and misuse*.

The principles outlined in 1973 are still applicable today, especially when considering the challenges facing identity systems, whether for use by the Federal government or by a commercial entity, that protect privacy and promote trust and transparency. These principles should be embraced by the policies, procedures, and governance that make up an identity system:

- Notice
- Choice
- Access
- Appeals
- Use limitation

The *notice* principle means that individuals who provide personal information to an enrollment process must receive proper *notice*. Notice refers to the information management practices that describe what data is collected, how it is used, to whom it is disclosed, and whether the information can be accessed or updated by the individual. Notice should be given before individuals provide their personal information. An example of this principle, the Gramm-Leach-Bliley Act requires the financial industry to provide customers with annual notification of information management practices.

The *choice* principle refers to an individual's ability to specify how information can be used once it is in the system, whether individuals can opt in or opt out of particular uses, and whether providing information is mandatory or voluntary.

The *access and appeals* principles refer to the ability of the individual to view personal or audit information held by an organization and to correct, update, or dispute the information. Access to personal information and formal appeals procedures are important policies, especially in circumstances in which information can be used to make negative determinations, such as disciplinary actions or credit-worthiness.

[1] *Records, Computers and Rights of Citizens*, Report to the Secretary's Advisory Committee on Automated Personal Data Systems, July 1973.

The principle of *use limitation* means the use of personal information must be limited to the purposes for which it was collected, unless individuals receive proper notification of additional uses.

Embedding Privacy Principles into an Identity Credential

There are technologies available today that can help promote the trust and transparency of identity systems by embedding privacy principles into the identity credential. Some of these technologies can be found in smart cards. For example, an identity credential stored in or generated by a smart card and used in combination with a password or personal identification number can ensure that information is only accessed or used for a valid purpose. Local (on-card) identity verification (that does not rely on a central database) lets individuals control when and where their information is accessed. And a smart card-based identity credential can also authenticate the information requestor, ensuring that personal information is only released to those authorized to access it.

Identity system owners and implementers can use smart card technology to help enforce the policies, procedures, and governance that support privacy and promote trust in identity management systems.

Identity Topic #9: Logical Access—Projecting Your Identity into the Online World

Using Identity to Reduce Online Risks

Industry, government, and consumers are increasingly looking to bolster a fundamental element of the trust chain—a person's identity—to help stem the threats of identity theft and online fraud. This increased focus on identity is intended to allow online and ecommerce systems to provide consumers with high-assurance identity services, such as mutual authentication, digital signatures, and enhanced auditing. These services hold the promise of improving consumers' overall online experience and reducing the threats associated with identity theft and online fraud.

Improvements in standards and technology have helped fuel the adoption of secure identity credentials, and are transforming the ways identity systems are viewed and used.

Improving Standards

In the past year, a number of new identity proofing and smart card standards have been published to help industry create products that are both practical to implement and easy to use. For example, the Personal Identity Verification (PIV) card specifications developed by the National Institute of Standards and Technology are standardizing the integration of identity management, smart cards, public key infrastructure (PKI), and biometrics. Additionally, financial industry guidance from the Federal Financial Institutions Examination Council (FFIEC) suggests the use of two-factor authentication for online banking. These have helped increase public awareness of the power of a secure identity credential.

As a result of this increase in public awareness and focus on standardization, businesses and consumers have more options for using identity credentials for numerous applications. For example, government agencies have deployed smart cards that enable employees to use one identity credential for physical access, network login, and access to online resources. This reduces the necessity to carry multiple tokens and remember multiple passwords.

As the ways in which an identity credential is used has expanded, so have the privacy policies that help ensure that users receive clear and concise information about how their identity information is used. The more robust these privacy policies are, and the better they are communicated, the more trust and confidence there will be in the identity system.

Maturing Technology and Standards = More User Options

Improved standards, increased awareness, and better privacy controls give consumers greater control and flexibility in creating and protecting their identities in cyberspace. The combination of secure identity technologies, maturing standards, and clear privacy controls is producing a wide array of options for users to safeguard their identities online. Technologies like the following are being used to build trust in identity systems and enhance the user's online experience:

- Smart cards – providing secure storage for identity information and digital keys
- Biometrics – binding individuals to their identity credentials conclusively
- One-time password generators – providing unique, one-time-use passwords
- Secure USB tokens – providing safe, easy-to-use storage for identity data

Building a Trust Chain

We now have the tools to create, transmit, and validate identity information securely and in a way that protects privacy. These tools can be used to establish a trust chain that can address some of the problems facing ecommerce and ebusiness today. These tools are allowing businesses and consumers to use identity credentials with more confidence, by granting more protection to all parties and ensuring that malicious users don't compromise identity relationships.

A Secure Future

Many identity systems are seeing the benefits of utilizing trusted identity credentials. And as usage of these tools and technologies increase, we can expect to see a compounding effect to their future adoption. For example, as governments further utilize smart card and biometric technologies as part of their identity standards, other industries are realizing benefits of lower costs, improved interoperability, and enhanced functionality. This transformation is already underway, as evidenced by computer manufacturers embedding smart card and biometric readers into their products, software vendors releasing smart card modules for popular operating system platforms and payment processors offering smart cards for fast and secure contactless payments. These and other emerging applications are giving businesses and consumers the opportunity to use their identity information in a safer, more secure, and more private environment.

Identity Topic #10: Biometrics—What Are They and How Do They Work?

Introduction

Biometric technology provides a unique and indisputable way to link a claimed identity to an actual person, and in so doing, improves the security, privacy, and trust in the overall identity management system.

A biometric is a physiological or behavioral characteristic that can be used to automatically recognize or verify a person's identity. Examples of some of today's commonly used biometrics include facial features, fingerprint patterns, iris patterns, hand geometry, and speech pattern analysis.

What is special about biometrics is that it is currently the only technology that can indisputably bind a person to an authentication or verification event. Other identity technologies, like ID cards or tokens, bind the event to the card or token but not necessarily to the person that it was rightfully issued to. Because biometrics utilize unique human characteristics, they are not easily lost, stolen, forged, or guessed.

How Are Biometrics Used to Prove Identity?

Three basic functions are typically performed when using biometrics. First is an initial enrollment, where the individual's biometric identifiers are captured and stored. Biometric data can be stored in a personal computer, in a network server, or in a smart card chip. Most biometric systems store only reduced digital elements of the biometric features rather than the original viewed image. This data is often referred to as a biometric template. Templates are a fraction of the size of the images from which they were derived. In most instances, a biometric template cannot be reversed to reconstitute the original image, thus protecting an individual's privacy.

Once an enrollment has been processed, verification, or one-to-one matching, can take place. Verification compares a presented biometric sample against a specific enrolled biometric template. This function verifies that the person is who the person claims to be. Individuals usually claim an identity through something that they have, like an ID card, or something that they know, like a username or number.

The third biometric function is identification, or one-to-many matching. Identification compares a presented biometric sample against a set of enrolled biometric templates. This process seeks to determine if a person is present or not present in the database.

How Are Biometrics Best Used in Identity Systems?

There is a wide range of proven biometric technologies available today, and each biometric can be applied to confirm personal identity accurately and reliably. However, some biometrics are better suited for certain applications than others.

Fingerprint biometrics measure the pattern and features associated with the friction ridges on a fingertip. Fingerprint biometrics are the most widely deployed because the technology is easy to use, very accurate, and very inexpensive to deploy. Fingerprint biometrics work well in either one-to-one verification or one-to-many identification.

The human face provides features and measurements of distance and angle that can be computed in two or three dimensions to determine a person's identity. While not as accurate as fingerprint technology, face recognition has significant benefits as an automated verification and identification tool. It uses a familiar digital photo process that most people are accustomed to and comfortable with. Face recognition can be performed from a distance without requiring the person to touch a biometric capture device.

Iris recognition measures the patterns of the iris, which is the colored area around the pupil of the eye. The iris is currently considered the most accurate biometric because significantly more information can be measured. Iris recognition can be accomplished from a distance of 1 to 3 feet and uses a low-intensity infrared light source, similar to that used in a television remote control. Iris recognition is increasingly popular in areas that require staff to wear gloves or other protective clothing that would interfere with fingerprint capture. Iris recognition is also being used for facility access and border control applications.

Hand geometry measures the length, thickness, and shape of the fingers on the hand. Hand geometry readers have been used for a number of years to protect access to high security areas in buildings. This technology can be deployed effectively in both indoor and outdoor environments and is typically used for verification (one-to-one matching) in conjunction with a card or personal identification number (PIN).

Vein pattern recognition is a relatively new biometric technology that uses light projected through a person's skin enabling a high-contrast matching of vein patterns in the fingers or hand area. The pattern of blood veins is unique to every individual, and apart from size, this pattern will not vary over the course of a person's lifetime. By measuring features beneath the skin, the pattern is much harder for others to observe, making vein recognition biometrics an especially secure method of verification.

Are There Limitations to Biometric Lifespan?

In general, biometric technologies in use today have a long useful lifespan, but some biometrics are more persistent and stable than others. Fingerprints are generally very stable but can be obscured due to skin damage from aging or occupational trauma. Iris patterns are formed very early in life and remain stable until death unless obscured by cataracts or other eye diseases. Face and hand geometry are less stable and persistent due to aging, weight change, and other factors. These issues can be overcome by periodic re-enrollment of the biometric characteristic.

Can Biometrics Be Combined or Used with other Authentication Methods?

Different biometrics can be combined to provide a higher level of assurance for extremely high security applications. It is more common, however, to combine a biometric with another authentication mechanism, such as a smart card or personal identification number (PIN). This concept of multi-factor authentication provides a layered approach that can enhance privacy and improve security. An identity system that utilizes smart cards and biometrics can significantly strengthen the chain of trust between a cardholder and a card issuer and reduce the risk and cost of identity theft and fraud. In such a system, the biometric is used as a secure key that unlocks the sensitive information stored on the smart card and activates the use of the card. If the card is lost or stolen, it is useless without the original cardholder’s unique biometric key.

How Mature Are Biometric Standards?

Biometric standards are quite mature. Since the early 1990s, the biometrics industry has been working closely with official standards-making bodies like the American National Standards Institute, the National Institute for Standards and Technology, and the International Organization for Standards to define standards that promote interoperability and uniform approaches to the implementation and testing of biometrics. Today, established standards include data interchange formats and application programming interface standards for biometrics as well as standards for using biometrics in secure financial transactions. These biometric standards continue to mature, largely driven by government actions to deploy biometrics for homeland security applications.

How Does Match-on-Card Provide Benefits for Offline Verification?

There are several ways to perform a biometric matching function. These include matching on a network server, on a computer, on a biometric capture device and on a smart card itself. The latter is called match-on-card, and provides a unique capability that leverages the security and computing power of the smart card. On-card matching enhances security by eliminating the need to transfer biometric information off the card for matching. On-card matching also eliminates the need for administering a separate centralized database of biometric templates thereby removing a potential privacy concern. This approach is also ideal for applications that have limited or no access to a network.

Biometric Technology – You Can't Leave Home without It

Biometric technology provides a unique capability to confirm personal identity. Each person receives biometric characteristics at birth and carries those biometric identifiers with them wherever they go. Because of this unique capability, biometric technology can be used to improve the security, enhance the privacy and build trust in the identity management systems of today and tomorrow.

Conclusions

The negative consequences of weak identity systems are well known. Identity theft causes serious financial losses for both individuals and businesses. Breaches in security and loss of identity data can be front-page news for businesses. Incorrect identity verification can compromise the nation's security systems. A lack of trust in individuals' identity credentials can compromise the trust on which many facets of modern life rely.

Society as a whole benefits when identity systems both provide individuals with a secure identity that others can trust and protect identity information through the entire life cycle of the information. Individuals benefit from being able to project an identity that is accepted and trusted, while knowing that the system is keeping their information private. Governments benefit from being able to verify individuals' identities accurately, thus allowing only authorized individuals to access privileges and services. Businesses benefit from being able to engage in trusted transactions and ensure that private information is protected.

Organizations must think through the entire identity process and chain of trust when they design and implement a secure identity system. A complete identity solution must include policies, procedures, and practices that implement the desired level of security and also describe how people interact with the system. The solution must start with accurate vetting of an individual's identity and continue with identity verification processes that provide secure, authorized access to identity information. Technology selection is also critical; technology in general, and smart cards and biometrics in particular, are powerful tools that can help achieve overall system goals and enforce adherence to privacy and security policies.

An increasing number of identity systems worldwide are using smart cards as one component of the identity solution. Smart cards are a vital link in the chain of trust for secure identity systems. They deliver unique capabilities for verifying cardholder identity securely and accurately, authenticating the identity credential, and serving the credential to the identity system. A strong business case now exists for smart card-based identity systems. Smart cards are affordable and provide security that cannot be obtained using typical identity authentication schemes. The standardization of hardware and software is driving down costs and increasing user acceptance, enabling smart cards to drive value in identity systems. As the smart card infrastructure becomes more pervasive, individuals also will reap greater benefits. From securely storing life-saving medical information to proving identity during travel to eliminating the need to carry cash, smart cards provide the mechanism to ensure that an individual's identity can be verified quickly and securely.

Biometric technology constitutes another valuable tool for establishing identity, since it is the only technology that can link a credential or event to a specific person. Biometrics are versatile and can be used for identity verification, matching a person against a specific record, or for identification, searching a database of biometric records for a match. Many identity systems combine biometric authentication with smart cards for higher levels of security. This multi-factor authentication approach combines something that a person has in their possession (the smart card) with something that they are (the biometric). Biometric implementations can now take advantage of established U.S. and international interoperability standards to provide flexibility and the widest possible technology choice.

The Smart Card Alliance Identity Council is working on projects to raise awareness of the issues that organizations face in implementing identity systems and to promote the use of the appropriate technologies to solve these issues. Secure, trusted identity systems will only result if complex policy, process, and technology issues are considered while new systems are being designed. The Council's goal is to provide guidance on these important identity issues, thereby helping both policy-makers and implementing organizations understand how smart card and related technologies can best be applied to deliver the benefits of secure identity.

The Identity Council welcomes input from government, businesses and the public. For additional information about Council activities, please visit [insert correct URL].

Publication Acknowledgements

This white was developed by the Smart Card Alliance Identity Council to raise awareness of the challenges that organizations face in implementing identity systems and to offer perspectives on how the top identity issues can be addressed with policy, process and technology solutions. Publication of this document by the Smart Card Alliance does not imply the endorsement of any of the member organizations of the Alliance.

The Smart Card Alliance wishes to thank the Identity Council members for their contributions. Participants involved in this project included: Axalto, Inc., Booz Allen Hamilton, Brightcard, Datacard Group, Fargo Electronics, Gemplus, Hitachi America Ltd., IBM, Identity Technology Partners (IDTP), International Biometrics Industry Association (IBIA), SafeNet, Saflink, Texas Instruments, Viisage, Visa USA.

Special thanks go to the individuals who wrote, reviewed, edited and contributed content to this white paper.

- **Gregory Abrenio**, Booz Allen Hamilton
- **Chuck Baggeroer**, Datacard Group
- **Kirk Brafford**, Saflink
- **Carla Dancy Smith**, Booz Allen Hamilton
- **Deanna Dicarlantonio**, Booz Allen Hamilton
- **Marty Dugan**, Viisage
- **Walter Hamilton**, Saflink, IBIA
- **Gary Klinefelter**, Fargo Electronics
- **John McKeon**, IBM
- **Cathy Medich**, Smart Card Alliance
- **Neville Pattinson**, Axalto
- **Ken Scheflen**, Viisage
- **Tres Wiley**, Texas Instruments
- **Chuck Wilson**, Hitachi America Ltd.

About the Smart Card Alliance Identity Council

The Identity Council is one of several Smart Card Alliance Technology and Industry Councils, a new type of focused group within the overall structure of the Alliance. These councils have been created to foster increased industry collaboration within a specified industry or market segment and produce tangible results while raising public awareness to the value of smart card technology.

The Identity Council is focused on promoting the need for technologies, legislation and usage solutions regarding human identity information to address the challenges of securing identity information, reducing identity fraud and increasing the usefulness that secure identity information delivers. The Council engages a broad set of participants and takes an industry perspective, bringing careful thought, joint planning and multiple organization resources to bear on addressing the challenges of securing identity information for proper use. The Council is currently working on projects to raise awareness of the issues that organizations and the public face in implementing and using identity systems and to promote the use of the appropriate technologies to solve these issues.

The Identity Council includes participants from across a broad spectrum of identity technology providers. Identity Council participation is open to any Smart Card Alliance member who wishes to contribute to the Council projects. Additional information about the Identity Council can be found at http://www.smartcardalliance.org.

Appendix I: Glossary

- **Access control.** The process of granting or denying specific requests to 1) obtain and use information and related information processing services; and 2) enter specific physical facilities (e.g., buildings, border crossing entrances).
- **Authentication.** The process of establishing confidence of authenticity; for example, the validity of a person's identity.
- **Biometric.** A measurable physical characteristic or personal behavioral trait used to recognize the identity or verify the claimed identity of an individual. Facial images, fingerprints, and iris scan samples are all examples of biometrics.
- **Biometric template.** The formatted digital record used to store an individual's biometric attributes. This record typically is a translation of the individual's biometric attributes and is created using a specific algorithm.
- **Breeder document**. A document used as an original source of identity to apply for (or breed) other forms of identity credentials.
- **Chain of trust**. An attribute of a secure ID system that encompasses all of the system's components and processes and assures that the system as a whole is worthy of trust. A chain of trust should guarantee the authenticity of the people, issuing organizations, devices, equipment, networks, and other components of a secure ID system. The chain of trust must also ensure that information within the system is verified, authenticated, protected, and used appropriately.
- **Contactless smart card.** A smart card that communicates with a reader through a radio frequency interface.
- **Credential.** Evidence attesting to one's right to a privilege (e.g., entering a building, crossing a border, getting government benefits). It is common for the term credential to be used to refer to the physical token, electronic information, or both.
- **Enrollment.** The process of entering the appropriate identity data for an individual into a system and associating the identity with the privileges being granted by the system.
- **ePassport.** A travel document that contains an integrated circuit chip that can securely store and communicate the ePassport holder's personal information to authorized reading devices.
- **Hacking**. The act of gaining illegal or unauthorized access to a computer system or network.
- **Identification.** The process by which the question "who is this person?" is answered. This function discovers the true identity of a person from an entire collection of similar persons. It requires a one-to-many match to locate the individual among the many individuals who are already enrolled in a system.
- **Identity.** An assortment of information that can be tied to an individual and that describes an individual's characteristics and uniqueness. Identity is information concerning the person, not the actual person.
- **Identity data.** The data associated with an individual's identity within a specific system and used by that system to verify the individual's identity.
- **Identity management system (IDMS).** System composed of one or more computer systems or applications that manages the identity registration, verification, validation, and issuance process, as well as the provisioning and deprovisioning of identity credentials.
- **Identity proofing.** The process of providing sufficient information (e.g., identity history, credentials, documents) to establish an identity to an organization that can issue identity credentials. Also known as identity vetting.

- **Identity theft.** The appropriation of another's personal information to commit fraud, steal the person's assets, or pretend to be the person.
- **Multi-factor authentication**. The use of multiple techniques to authenticate an individual's identity. This usually involves combining two or more of the following: something the individual has (e.g., a card or token); something the individual knows (e.g., a password or personal identification number); something the individual is (e.g., a fingerprint or other biometric measurement).
- **Pharming**. A cyber attack that directs people to a fraudulent website by poisoning the domain name system server.
- **Phishing**. A cyber attack that directs people to a fraudulent website to collect personal information for identity theft.
- **Public key infrastructure (PKI).** A support service that provides the cryptographic keys needed to perform digital signature-based identity verification and protect communication and storage of sensitive verification system data within identity cards and the verification system.
- **Secure identity.** The verifiable and exclusive right to use the identity information being presented by an individual to access a set of privileges
- **Skimming**. The practice of stealing credit card numbers by capturing the information in a data storage device.
- **Smart card.** A device that includes an embedded integrated circuit that can be either a secure microcontroller or equivalent intelligence with internal memory or a memory chip alone. The card connects to a reader with direct physical contact or with a remote contactless radio frequency interface. With an embedded microcontroller, smart cards have the unique ability to store large amounts of data, carry out their own on-card functions (e.g., encryption and digital signatures) and interact intelligently with a smart card reader. Smart cards are available in a variety of form factors, including plastic cards, subscriber identification modules used in GSM mobile phones, and USB-based tokens.
- **Token**. A physical device that carries an individual's credentials. The device is typically small (for easy transport) and usually employs a variety of physical and/or logical mechanisms to protect against modifying legitimate credentials or producing fraudulent credentials. Examples of tokens include picture ID cards (e.g., state driver's licenses), smart cards, floppy disks, and memory sticks.
- **Verification**. The process by which the question "is this person who the person claims to be?" is answered. This function requires a one-to-one match between presented identity information and identity information that is known to a system.